REMARKS

Applicant has amended claims 19, 20, 23, 24, 26, 30, and 36. Applicant respectfully traverses the following rejection made in the Final Office Action: rejection of claims 19-36 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent App. Pub. No. 2005/0055391 ("*Carlson*") in view of U.S. Patent No. 5,383,143 ("*Crouch*").

Rejection of Claims 19-36 under 35 U.S.C. § 103(a):

Applicant requests reconsideration and withdrawal of the rejection of claims 19-36 under 35 U.S.C. § 103(a) as being unpatentable over *Carlson* in view of *Crouch*.

The Final Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective obviousness analysis. *See* M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 U.S.P.Q.2d 1385 (2007).

In particular, the Final Office Action has not properly determined the scope and content of the prior art, at least because the Final Office Action incorrectly interpreted the content of *Carlson* in view of *Crouch*. In addition, the Final Office Action has not properly ascertained the differences between the claimed invention and the prior art, at least because the Final Office Action has not properly interpreted the prior art and considered _both_ the invention _and_ the prior art _as a whole_. *See* M.P.E.P. § 2141(II)(B).

Independent claim 19 recites, in part, "a true random number generator," "a pseudo-random number generator," and "a mixing logic connected between said true

random number generator and said pseudo-random number generator" (emphasis added). *Carlson* fails to teach or suggest at least these elements.

Specifically, *Carlson* teaches an "RNG 100 compris[ing] an entropy generator 101 and a mixing function 152." *Carlson*, par. [0018]. In *Carlson*, the "entropy generator 101" comprises "a set of one or more oscillators 105A-105N" and a "LFSR 130." *Carlson*, par. [0018]; *see also* Fig. 1. The Final Office Action asserts that the "entropy generator," the "linear feedback shift register (LFSR) [1]," and the "mixing function" of *Carlson* correspond to the claimed "true random number generator," the claimed "pseudo-random number generator," and the claimed "mixing logic," respectively. *See* Final Office Action, p. 3, and *also* Advisory Action, p. 2, pars. 1-2.

However, Fig. 1 of *Carlson* clearly shows that the mixing function 152 does not output anything to either the entropy generator 101 or the LFSR 130. Rather, the mixing function merely receives the output of the LFSR 130 and generates a robust random number 152. In view of this, the mixing function 152 of *Carlson* is <u>not</u> connected between the entropy generator 101 and the LFSR 130.

For at least the reasons noted-above, *Carlson* fails to teach or suggest at least "a mixing logic connected <u>between</u> [a] true random number generator and [a] pseudo-random number generator" as recited in claim 19 (emphasis added).

Crouch fails to cure the deficiencies of *Carlson*. The Final Office Action admits that "Carlson does not expressly teach the claim [] element of a pseudo-random generator," but asserts that *Crouch* teaches "the use of a pseudo-random number

---

[1] The Final Office Action reads "a Left Shift Register." Final Office Action, p. 3. However, Applicant respectfully submits that there is no such term used in *Carlson*. The Advisory Action states that *Carlson* "describes a LFSR." Advisory Action, p. 2, par. 5. Applicant respectfully notes that "LFSR" in *Carlson* stands for "Linear Feedback Shift Register." *See*, e.g., *Carlson*, par. [0008]. Therefore, Applicant reasonably believes, and the Examiner appears to acknowledge, that "a Left Shift Register" in the Final Office Action is a typographical error of "a Linear Feedback Shift Register."

generator [to] provide the capability to create a random number using a pseudo-random generator." Final Office Action, p. 4. Even if this assertion is correct, to which Applicant does not concede, *Crouch* nevertheless fails to teach or suggest the claim features quoted and discussed above.

Moreover, Applicant respectfully traverses the assertion in the Advisory Action that "applicant's claim 19 as argued reads different th[a]n as claim[ed]." Advisory Action, p. 2, par. 7. Applicant respectfully notes that claim 19, as prior to amending, recited, in part, that "a generator of <u>an alteration signal intended to change the behavior of said pseudo-random number generator</u> . . . said generator of the alteration signal being connected so as to receive said seed and <u>generate said alteration signal</u> by <u>processing said seed by means of the sequence generated by said pseudo-random number generator</u>." Therefore, claim 19 as previously amended and argued did not read different than as claimed. *See* the Request for Reconsideration after Final filed December 28, 2009.

Notwithstanding the above, however, Applicant has amended claim 19 for clarification. Claim 19, as amended, further recites that "said mixing logic compris[es] an alteration signal generator generating an alteration signal . . . altering the behavior of said pseudo-random number generator at multiple random instants . . . thereby obtaining . . . multiple pseudo-random sequences of random lengths" and "said alteration signal generator . . . generating said alteration signal based on said seed and said pseudo-random sequence." *Carlson* also fails to teach or suggest these elements.

As discussed above, the mixing function 152 of *Carlson* only receives output from the entropy generator 101 or the LFSR 130, but does not output anything to either the entropy generator 101 or the LFSR 130. In view of this, there is no such a

-10-

generator in the mixing function 152 of *Carlson* (as allegedly corresponding to the claimed "mixing logic") to generate an alteration signal to alter the behavior of the LFSR 130 (as allegedly corresponding to the claimed "pseudo-random number generator").

The Advisory Action asserts that *Crouch* "teaches the ability of receiving a seed value to alter the behavior of a pseudo-random number generation sequence." Advisory Action, p. 2, par. 7. However, this assertion is not correct.

Specifically, *Crouch* teaches "generat[ing] . . . pseudo-random values . . . by re-seeding (i.e., <u>replacing</u> an old seed with a new seed . . . selected from a pseudo-random number generated by the LFSR [] using the old seed)." *Crouch*, col. 5, ll. 20-25, (emphasis added). Thus, in *Crouch*, when generating new pseudo-random values, the old seed is not used. Accordingly, *Crouch* fails to teach or suggest "generating [an] alteration signal [altering the behavior of said pseudo-random number generator] <u>based on said seed and said pseudo-random sequence</u>" as recited in claim 19 (emphasis added).

In addition, *Crouch* teaches choosing a new seed after a <u>fixed</u> number of clock cycles and all such-generated pseudo-random sequences have the <u>same fixed</u> length. *See, e.g., Crouch*, col. 5, l. 45 - col. 6, l. 36. Thus, *Crouch* also fails to teach or suggest "altering the behavior of said pseudo-random number generator at multiple <u>random</u> instants . . . thereby obtaining . . . multiple pseudo-random sequences of <u>random</u> lengths" as recited in claim 19 (emphases added).

In view of the above, *Crouch* fails to cure the deficiencies of *Carlson*. For brevity, Applicant's arguments regarding *Crouch* as presented in the Amendment filed on June 3, 2009 are maintained and incorporated by reference.

Moreover, in response to the Amendment filed June 3, 2009, the Final Office Action states that "[t]he Examiner does not fully understand why applicant's arguments are pertaining to Crouch's capability to produce a "true random number" using a random number generator." Final Office Action, pp. 21-22. In addition, the Advisory Action states that "[w]ith regards to applicant remarks pertaining to Crouch['s] ability to generate a random number, the Examiner respectfully submits figure 6 of Crouch describes such capability." Advisory Action, p. 2, par. 9. However, Applicant again respectfully notes that the arguments in the above-noted Amendment are <u>not</u> pertaining to *Crouch*'s *capability* to produce a "true random number" or a "random number." Rather, the arguments are that "[t]he first seed [used by the pseudo random number generator of *Crouch*] is not a "true random number" . . . but [] is [] stored in memory or generated by a deterministic process." *See* Amendment of June 3, 2009, p. 9.

Finally, Applicant acknowledges the Final Office Action's statement that "[w]ith regards to applicant's "non-consideration of claim[ed] subject matter" argument presented in applicant's remarks in pg. 10, on 6/3/2009, the Examiner contends the subject matter omitted was done by accident." Final Office Action, p. 22. In response, Applicant's arguments at pp. 8-10 of the Amendment filed on June 3, 2009 are incorporated by reference. Applicant notes that independent claim 19 is <u>not</u> a product-by-process claim, despite the allegation in the Final Office Action at p. 22, and all features recited in claim 19 should be given patentable weight during examination. Therefore, the Examiner's response to Applicant's previous arguments is insufficient.

Therefore, independent claim 19 is not obvious over *Carlson* and *Crouch*, whether taken alone or in combination, and thus should be allowable. Independent claim 30, although different in scope from independent claim 19, recites elements

similar to those of claim 19. Therefore, at least for reasons similar to those discussed above, claim 30 is also not obvious over *Carlson* and *Crouch*, whether taken alone or in combination, and thus should be allowable. Dependent claims 20-29 and 31-36 are also allowable at least by virtue of their respective dependence from base claim 19 or 30, and because they recite additional features not taught or suggested by the cited references. Therefore, Applicant respectfully requests withdrawal of the rejection.

Conclusion:

Applicant respectfully requests reconsideration of the application and withdrawal of the rejection. Pending claims 19-36 are in condition for allowance, and Applicant respectfully requests a favorable action.
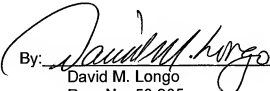
If there are any remaining issues or misunderstandings, Applicant requests the Examiner telephone the undersigned representative to discuss them.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account no. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 25, 2010

By: _David M. Longo_
David M. Longo
Reg. No. 53,235
/direct telephone: (571) 203-2763/